View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Institute of Advanced Engineering and Science

International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 6, December 2020, pp. 6039~6044
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i6.pp6039-6044

A risk and security assessment of VANET availability using attack tree concept

Meriem Houmer, Moulay Lahcen Hasnaoui
Information and Communication Systems Engineering Research Team,
Mathematical Modeling and Computer Science Laboratory, National Graduate School of Arts and Crafts,
Moulay-Ismail University, Morocco

Article Info

Article history:

Received Mar 16, 2020
Revised May 11, 2020
Accepted May 23, 2020

Keywords:

Attack-tree
Availability
Risk assessment
Security
VANET

ABSTRACT

The challenging nature of insecure wireless channels and the open-access environment make the protection of vehicular ad hoc network (VANET) a particularly critical issue. Robust approaches to protect this network's security and privacy against attacks need to be improved, trying to achieve an adequate level, to secure the confidential information of drivers and passengers. Accordingly, to improve the security of VANET, it is necessary to carry out a risk assessment, in order to evaluate the risk this network is facing. This paper focuses on the security threats in VANET, particularly on the availability of this network. We propose a novel risk assessment approach to evaluate the risk of the attack against VANET availability. We adopt a tree structure called attack-tree to model the attacker's potential attack strategies. Based on this attack-tree, we can estimate the probability that a specific menace might lead against VANET and detect potential attack sequences that an attacker could launch against VANET availability. Then, we utilize the utility multi-attribute theory to measure the total risk value of the system, including the probabilities of each sequence of attack. The analysis results of the study will help decision-makers take effective precautions to prevent attack on this network's availability.

Copyright © 2020 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Meriem Houmer,
Information and Communication Systems Engineering Research Team,
Mathematical Modeling and Computer Science Laboratory,
National Graduate School of Arts and Crafts, Moulay-Ismail University, Meknes, Morocco
Email: houmer.m@gmail.com

1. INTRODUCTION

The technological development has reached all domains, especially the communications area, which is undergoing major changes in wireless technology advent. This technology was used by researchers to permit vehicles to interact with each other, with or without infrastructure installed next to the road, which constitutes the networks called Vehicular Ad-Hoc NETwork (VANET).

VANET constitutes the core of the intelligent transport system (ITS) having as main objective the improvement of road safety [1] by taking advantage of the emergence of communication technology and the lowering of the cost of wireless devices. Indeed, thanks to sensors installed in vehicles, or located next to the roads and control centers, vehicle communications will allow drivers to be warned early of possible dangers [2]. In addition, these networks will not only improve road safety but will also offer new services to road users [3], making road use more pleasant. Interesting contributions regarding the exchange of information between vehicles have been proposed recently in several research projects related to road safety.

Typically, the destination vehicle utilizes the information sent by the source vehicle in order to better analyze the situations of the road that arise. This situation can give rise to security attacks by adversaries. Due to the importance of vehicle-to-vehicle exchanges and openings of the VANET

environment, many attackers can send alerting messages whose content is falsified or prevent a legitimate message being delivered in order to cause accidents [4]. They can prevent the routing of these messages by attacking the network availability in order to make this network unavailable, and then its main goal will become useless.

Our research work aims to ensure the vehicle system's reliability. In order to develop counter measures against threats led by adversaries, it is necessary to analyze and minimize possible attacks against the system's assets. Our analysis of the attack is based on a structure and decision tree called the attack-tree. According to the attack-tree method, we suggest a new risk assessment approach for VANET availability. Attack-tree based risk analyzes use a tree-based approach to model and evaluate system risk and define possible attack strategies that the attacker can lead against this system. Using this approach, the capacity of the attack source can be analyzed and the degree of the effects of attacks led against the network can be estimated. Taking advantage of the attack-tree method, in this paper, we use it to identify the possible threats launched against VANET availability, and we measure further the overall likelihood of the attacker hitting the target goal. Finally, the decision-maker will decide which measures of protection will be implemented based on the quantitative result.

The rest of this paper is structured as follows: Section 2 presents the attack-tree fundamentals. Section 3 introduces the attack-tree model for VANET availability. The risk assessment is analyzed in section 4. Finally, we conclude in section 5.

2. ATTACK TREE FUNDAMENTALS

2.1. Definition

Bruce Schneier [5, 6] has described the attacks trees as a model of threats led against systems. It is an analytical technique in which the system is analyzed from the attacker's point of view in order to find all credible ways in which the attack event can occur. However, when we consider all the different techniques in which a system may be attacked, we will possibly establish the safest countermeasures to avoid such attacks. Attack trees are used in a variety of contexts, such as safety and aerospace, in order to analyze and evaluate attacks against the tamper-resistant electronics system. In addition, they have been used in the field of information technology to analyze attacks against sensors and computer systems and interpret the convenient method by which an attacker can carry out a specific attack [7].

Basically, every node in the attack-tree indicates a particular threat. At top of the tree, we find the root node which represents the global objective of the attacker. The other nodes which are the leaves of the tree represent sub-objectives. Generally, a binary relation (also called operator) is associated with the internal nodes of the tree. These operators can be AND or OR. An AND operator (respectively an OR operator) is considered successful when all of its child nodes (respectively, at least one) are successful. There are different kinds of attack trees such as Defense-tree [8], Protection-tree [9], Attack-defense trees [10], and Vulnerabilities-Tree [11]. They have the same attack-tree characteristics, few aspects which distinguish them.

2.2. Attack tree basis

An attack tree is a technique of evaluating network security against its probable attacks. However, we use an attack tree to interpret attacks that an external intruder or insider attacker can generate in a communications network. Attack trees allow us to measure security risks that face a system with regard to losses caused by attacks [12] or the benefit of defenders through the usage of defense security mechanisms. The analysis of a network or a system through this technique contributes to the estimation of a probabilistic risk assessment of the network that facilitates communication systems growth. Initially, the fundamental attack tree does not provide defense mechanisms.

The mechanism used in constructing the attack tree is structured to define the sequence of events leading to the definitive event chosen (root node). The root node in the tree represents the global goal of the attacker, and leaf nodes represent the sub-goals. The attack goal must be carefully selected. In addition, we may have several root nodes reflecting different goals in complex systems. Nodes can be connected, particularly, through AND and OR Boolean operators [13]. These operators are considered as the basic gates to construct the attack tree. The OR gate describes the different manners to attain the same goal (the attack goal may be attained by reaching the first OR the second leaf nodes), while AND gates depict the different ways toward the same goal goal (the attack goal may be attained by reaching the first AND the second leaf nodes).

Eventually, during the construction of the attack tree it is important to ensure that the structure is consistent and to comply with some extra rules which are:

- Any element failure induces system failure.

- The successful implementation of all its elements guarantees that the system operates correctly.
- When the system fails, the system does not resume service due to a novel attack.
- If the mechanism functions correctly, abduct an attack from the system does not cause its failure. It can happen that an attack on an element reduces or remove the impact of an anterior attack and thus allow the functioning of the system.
- Be sure to identify all logical gate's input events before determining their corresponding causes.
- Avoid linking directly two logical gates.
- Choose anterior causes just before the event exists.

On the basis of the above, we designed vehicular ad hoc network attack tree model and selected a range of major privacy issues as targets for the attacker. The availability of vehicular network represents the attacker's goals [14]. The next section includes a stepwise analysis for building our attack tree.

3. BUILDING ATTACK TREE FOR VANET AVAILABILITY

In order to construct our attack tree, we opt for a step-by-step refinement model. However, VANET availability is the global goal of the attacker and the root node of our attack-tree. This goal is indicated by G as shown in Figure 1. The attack tree construction process involves the following steps:

- Identify the global goal (root node) of the attacker: VANET availability (G).
- Divide the global goal "VANET availability" within sub-goals. In our case, there are three leaves attached to the root node: Black Hole (S1) [15], Denial of Service (S2) [16], Malware & spam (S3). If only one of the sub-goals is reached, the goal of the attacker will be accomplished. It is possible to extend this list and add several sub-targets. The list of sub-goals could be extended and other sub-goals might be included.
- In the following step, we continue the building of the different elements (leaves) of our attack three models:

a. The first sub-goal "black hole" can be reached by combining two-element: cheat the routing protocol (E1) and establish a forged route (E2)

In a black hole attack, the routing protocol is tricked by a malicious node in order to have a brief route to the target node. Once a pathway is created between the spiteful node and the target node, the attacker can remove incoming and outgoing traffic without informing the source that the packets sent have not reached their destination. Moreover, the attacker can forward the packets anywhere they want [17].

b. Denial of Service (S2) represents the second sub-goal

The denial of service or DoS is an attack in which the attacker aims to make a server, service, or infrastructure inaccessible for an undefined duration. This sub-goal can be achieved through:

Channel jamming (S21): the attacker's goal, through channel jamming, is to block nodes from reaching network services. This objective can be achieved by transmitting dummy messages (E3) in which the attacker transmits various messages to the other vehicles using fake identities. Through transmitting dummy messages, the attacker can attain his main goal that consists of decreased the reliability and efficiency of the network, furthermore, forcing certain vehicles to exit the roads for his own benefit [18]. Channel jamming may also be obtained by broadcasting high-frequency signals (E4). This task involves the attacker transmitting request messages with higher frequency, which induces a system failure. Consequently, other nodes cannot receive or transmit packets in network [19].

Smurfing (E5): The smurf technique uses the broadcast servers to paralyze the network. This server is capable to duplicate messages and sending it to all nodes on the same network. Actually, the malicious node sends a ping request to one or more broadcast servers by falsifying the source IP address and by providing the IP address of a target machine [20]. Then, the broadcasting server passes on the request to the entire network. All nodes on the network send a response to the broadcasting server. Finally, the broadcast server redirects responses to the target machine. Moreover, when the malicious node sends a request to several broadcast servers located on different networks, all the responses from the nodes on the different networks will be routed to the target machine. In this way, most of the attacker's job is to find a list of broadcast servers and falsify the reply address in order to direct them to the target machine.

Flooding (S22): this technique consists of sending a large quantity of useless data in the network in order to make it unusable, for example by saturating its bandwidth or by causing the nodes of the network to crash, whose denial of service is the possible consequence. This attack can be carried out with two tasks: SYN flood (E6) or UDP flood (E7) [21].

The SYN flood [22] aims to saturate a server by sending a multitude of TCP packets in order to overwhelm the target server with SYN (Synchronized) requests en masse. This will aim to create

a multitude of connections requiring a large number of system resources. The target is then overwhelmed by these requests and can no longer respond to legitimate requests.

Like the SYN flood, in the UDP flood, the attacker transmits several UDP requests to the targeted system in order to overwhelm it. Unlike TCP transmission, data can be transferred via UDP without the need for an established connection. As UDP traffic takes priority over TCP, it may quickly interrupt and saturate the network traffic.

c. The final sub-goal is malware and spam (S3)

Malicious software (Malware) is a program developed by malicious to damage a computer system or access to the private personal information, without the consent of the user or the target node that is infected. Otherwise, in spam messages, the attacker forwards several unsolicited emails to an address in order to overload its mailbox and that to scattered the attention of the user from important messages [21]. To reach this sub-goal (S3), it is requisite to carry out: a) Inserted viruses and worms (E8) in a reliable program by including a clone of itself and being part of it, b) Through submitting spam messages, the attacker uses the quota that is available in an e-mail service to prevent legitimate messages from being sent.

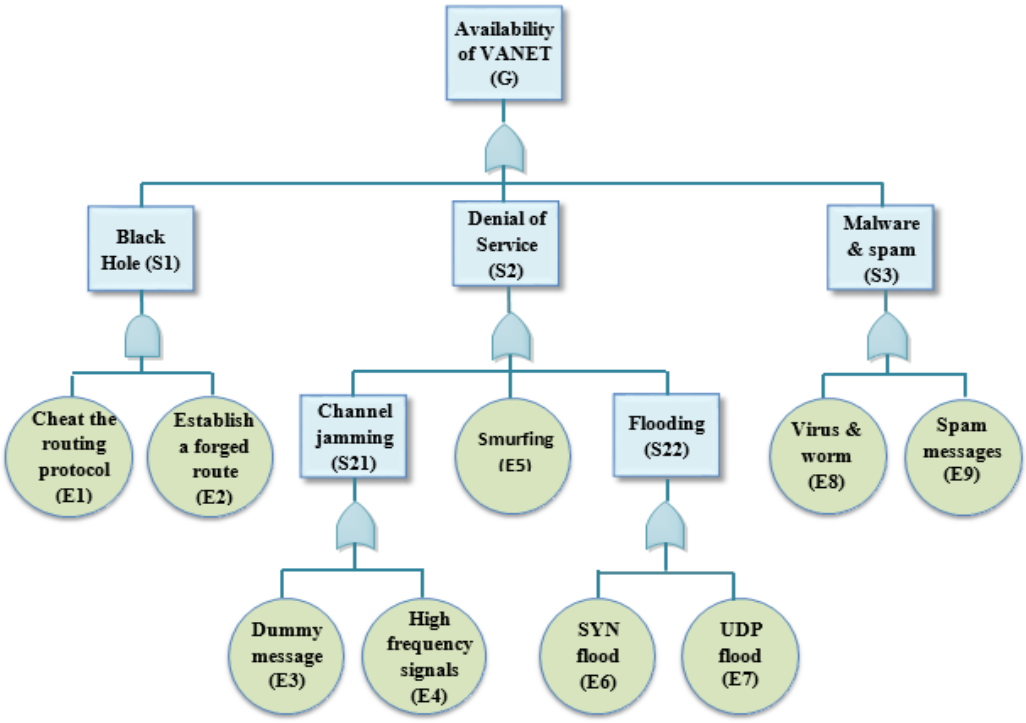

Figure 1. Attack tree model for VANET availability of the network

4. RISK ASSESSMENT

The attacker needs to consider various features containing the attack cost, technique difficulty, and the possibility of being discovered. The main objective is to assign values to each node in the attack tree. In this work, we regard three attributes of the leaf nodes which are: attack cost c_L , technical difficulty d_L, and the discovering difficulty s_L. The grade-level standards are illustrated in Table 1. Those values are attributed to leaf nodes depending on the measures cited in [23]. We use the multi-attribute utility theory [24] in other to relocate these features into attackers' utility value P_L, which is the probability of a leaf node occurring. Formula (1) is used to calculate each leaf node's utility.

$$P_L = w_1 \times u_{(c_L)} + w_2 \times u_{(d_L)} + w_3 \times u_{(s_L)} \quad (1)$$

where $u_{(c_L)}$, $u_{(d_L)}$, $u_{(s_L)}$ are the utility function of c_L, d_L and S_L respectively, and their values are confined between [0,1]. w_1, w_2, w_3 are the weights of the utilities where: $w_1 + w_2 + w_3 = 1$. So, we can admit that $w_1 = w_2 = w_3 = 1/3$, and we suppose that $u_{(c_L)} = u_{(d_L)} = u_{(s_L)} = u_{(x)} = c/x$ (where c = 0.2).

Table 2 presents the probability P_L that each leaf node will occur. Furthermore, the attack tree is converted to binary decision diagram (BDD) [25] in other to compute the overall probability of achieving the objective of the attack. This probability equals 0.2336.

Table 1. Grade standard

Attack cost (c_L)	Technical difficulty (d_L)	Discovering difficulty (s_L)	Grade
>10	Quite difficult	Quite simple	5
6 – 10	Difficult	Simple	4
3 – 6	Mediate	Mediate	3
0.5 – 3	Simple	Difficult	2
<0.5	Quite simple	Quite difficult	1

Table 2. Attribute values for leaf nodes and its occurrence probability

Leaf node	Attack cost (c_L)	Technical difficulty (d_L)	Discovering difficulty (s_L)	Occurrence probability (P_L)
E_1	3	4	1	0.105
E_2	3	2	1	0.122
E_3	5	2	5	0.06
E_4	2	3	4	0.072
E_5	5	1	3	0.102
E_6	4	2	3	0.072
E_7	4	2	3	0.072
E_8	2	1	4	0.116
E_9	3	4	2	0.072

After that, we are constructing the attack sequences depending on our attack-defense tree. The sequences of the attack are a real path consisting of a leaf node group. Only when all attack sequence events occur, the attacker can achieve his final objective. When the attack sequences were known, their occurrence probabilities can be calculated and then compared to find which attack sequence the attacker could most probably launch. An attack sequence is described as:

$$S_i = (E_1, E_2, \dots, E_n)$$

So, the probability of an attack sequence is:

$$P_S(S_i) = P(E_1) \times P(E_2) \dots \times P(E_n) \quad (2)$$

In order to obtain all attack sequences for our attack-defense tree, we use the Boolean algebra method. The attack sequences to attain the attack goal are:

S1={E1,E2}, S2={E3}, S3={E4}, S4={E5}, S5={E6}, S6={E7}, S7={E8}, S8={E9}.

The first sequence $\{E_1, E_2\}$ imply that the adversary can make the network unavailable by cheating the routing protocol (E_1) and Establish a forged route (E_2), but in the second sequence, the attacker requisite just through transmit dummy messages (E_3) and so on. Based on the (2), we compute the attack sequences occurrence probabilities which are shown in Table 3. From Table 3, we can deduce that the attack sequence S7 is the most probable path to occur. Thus, to keep the network protected we should focus on this attack.

Table 3. Occurrence probabilities of attack sequences

Attack sequence	Occurrence probability (P_S)
S_1	0.0128
S_2	0.06
S_3	0.072
S_4	0.102
S_5	0.072
S_6	0.072
S_7	0.116
S_8	0.072

5. CONCLUSION

In this paper, we are proposing a new security analysis method based on the attack-tree to analyze the risk of VANET availability from a system point of view. Furthermore, we are constructing an attack tree with VANET availability leakage as the global objective to analyze the behavior of the attacker. To measure the system risk, we are assigning values to all leaf nodes of the tree and adopt the multi-attribute utility method so the assessment would be more analytical. Based on the analysis of the attack sequences, we recognize the most probable path that the attacker might select. In our future work, we will present a VANET privacy and security risk assessment based on the attack-defense tree model. That model analyzes the defense strategies of the system.

REFERENCES

[1] T. O. Fahad, A. A. Ali, "Compressed fuzzy logic based multi-criteria AODV routing in VANET environment," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no.1, pp. 397-401, 2019.

[2] O. Mahma, et al., "An Efficient Broadcast Protocol for Warning Message Dissemination in VANETs," *Journal of computing and information technology*, vol. 26, no. 3, pp. 157-166, 2018.

[3] P. Nivetha, and S. Muruganantham, "Leverageing Route Saving in Location Based Services on VANET Using KNN," *International Journal of Engineering Science*, pp. 3179-3183, 2016.

[4] C. K. Karn and C. P. Gupta, "A survey on VANETs security attacks and Sybil attack detection," *International Journal of Sensors Wireless Communications and Control*, vol. 6, no. 1, pp. 45-62, 2016.

[5] B. Schneier, "Attack Trees," *Dr. Dobb's Journal of Software Tools*, vol. 24, no. 12, pp. 21-29,1999.

[6] B. Schneier, "Secrets and Lies: Digital Security in a Networked World," *John wiley & Sons*, 2015.

[7] S. Mauw and M. Oostdijk, "Foundations of Attack Trees," in *International Conference on Information Security and Cryptology*, pp. 186-198, 2005.

[8] S. Bistarelli, et al., "Strategic games on defense trees," in *International Workshop on Formal Aspects in Security and Trust, Springer*, pp. 1-15, 2006.

[9] Y. Li, et al., "On Finding the Multicast Protection Tree Considering SRLG in WDM Optical Networks," *Electronics and Telecommunications Research Institute*, vol. 28, no. 4, pp. 517-520, 2006.

[10] B. Kordy, et al., "Foundations of Attack–Defense Trees," in *International Workshop on Formal Aspects in Security and Trust*, pp. 80-95, 2010.

[11] S. Vidalis and A. Jones, "Using Vulnerability Trees for Decision Making in Threat Assessment," in *2nd European Conference on Information Warfare*, 2003.

[12] M. Cremonini and P. Martini, "Evaluating information security investments from attackers perspective: the return-on-attack (ROA)," in *WEIS*, pp. 1-3, 2005.

[13] R. Kumar, et al., "Quantitative attack tree analysis via priced timed automata," in *International Conference on Formal Modeling and Analysis of Timed Systems*, pp. 156-171, 2015.

[14] S. Du and H. Zhu, "Security Assessment via Attack Tree Model," *Security Assessment in Vehicular Networks*, pp. 9-16, 2013.

[15] N. Panda and B. K. Pattanayak, "Analysis of Blackhole Attack in AODV and DSR," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3092-3102, 2018.

[16] W. Ahmed and M. Elhadef, "DoS attacks and countermeasures in VANET," *International Conference on Future Information Technology*, pp. 333-341, 2018.

[17] V. Bibhu, et al., "Performance Analysis of Black Hole Attack in Vanet," *International Journal Computer Network and Information Security*, vol. 4, no. 11, pp. 47-54, 2012.

[18] H. Hasbullah, et al., "Denial of service (DOS) attack and its possible solution in VANET," *International Journal of Electronics and Communication Engineering*, vol. 4, no 5, pp. 813-817, 2010.

[19] S. A. Yah, et al., "Newton-raphson method to solve systems of non-linear equations in VANET performance optimization," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no 1, pp. 336-342, 2019.

[20] S. Specht and R. Lee, "Taxonomies of distributed denial of service networks, attacks, tools and countermeasures," CEL 2003-03, Princeton University, Princeton, NJ, USA, 2003.

[21] M. Houmer, et al., "Security Analysis of Vehicular Ad-hoc Networks based on Attack Tree," in *2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, pp. 21-26, 2018.

[22] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study," *International Journal of Security and Its Applications*, vol. 10, no. 5, pp. 261-274, 2016.

[23] R. Jiang, et al., "An attack tree based risk assessment for location privacy in wireless sensor networks," in *8th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2012.

[24] A. Ishizaka and P. Nemery, "Multi-attribute utility theory," *Multi-Criteria Decision Analysis: Methods and Software*, 2013.

[25] S. Yan, "A research on variable ordering methods of binary decision diagram," Master's Thesis, Shanghai JiaoTong University, Shanghai, 2008.